



IN THE MISSOURI COURT OF APPEALS WESTERN DISTRICT

KENNETH SHUMATE,)	
)	
Appellant,)	
)	
vs.)	WD79486
)	
STATE OF MISSOURI,)	Opinion filed: March 28, 2017
)	
Respondent.)	

APPEAL FROM THE CIRCUIT COURT OF GENTRY COUNTY, MISSOURI THE HONORABLE ROGER M. PROKES, JUDGE

Before Division Three: Victor C. Howard, Presiding Judge,
Gary D. Witt, Judge and Zel Fischer, Special Judge

Kenneth Shumate appeals the judgment of the motion court denying his Rule 29.15 motion for postconviction relief without an evidentiary hearing. Shumate sought to vacate his convictions following a bench trial of three counts of first-degree statutory sodomy, six counts of second-degree statutory sodomy, two counts of second-degree statutory rape, and one count of sexual exploitation of a minor and consecutive sentences of three terms of life imprisonment plus fifty-five years. He claims that he received ineffective assistance of counsel when counsel failed to move to suppress all evidence obtained as a result of the warrantless search of the United States Internet Crimes Against Children database that provided law enforcement officers his IP address despite lack of prior individualized probable cause. The judgment is affirmed.

Background

In the spring of 2012, law enforcement officers suspected that a particular IP (Internet Protocol) address was sharing child pornography. The officers served an investigative subpoena to the Internet service provider to obtain the name and address of the subscriber for the IP address, which identified Shumate. After unsuccessfully trying to download files offered for sharing directly from Shumate's IP address, officers decided to make contact with him at his home on September 25, 2012. The officers explained that they were conducting an investigation involving the downloading of child pornography and asked Shumate if he had any knowledge of such. Shumate told the officers that he had two laptops and Internet service and that he downloaded adult pornography but not child pornography. Shumate and his wife consented to an examination of the laptops by the officers. The officers found several pornographic pictures of a female they believed to be about fourteen years old. They also found a website open to a story involving sexual relations with children. At that point, the officers seized the computers so that they could apply for a search warrant to conduct computer forensic examinations. A warrant was issued, and forensic examinations of the computers found images of sexual encounters between Shumate's wife and his minor son. Shumate was arrested, a search of his house and car recovered a thumb drive and camera, and his two minor sons were interviewed, which led to the statutory sodomy, statutory rape, and exploitation charges.

Before trial, defense counsel filed a motion to suppress any items seized from the Defendant's person and/or residence on or about the 25th day of September, 2012 and thereafter including but not limited to Shumate's HP Pavillion laptop, his wife's HP laptop, all evidence seized from the computers, the recorded interviews of the child victims, and the testimony of law enforcement officers regarding evidence viewed as a result of the unlawful search and seizure

including statement made to them by Shumate. Defense counsel generally alleged that the search and seizure violated the United States and Missouri Constitutions because they were made without a valid warrant and without lawful authority.

At the evidentiary hearing on the motion to suppress, the State presented the testimony of Detective Steve Feeney of the Kirksville Police Department. Regarding the issue in this case, Detective Feeney testified that he is a member of the Missouri Internet Crimes Against Children (ICAC) task force that conducts online investigations throughout the state of cases involving child pornography, child enticement, and sexual abuse of children. The State is divided into 61 task forces by geographical location with Detective Feeney's task force covering thirteen counties in Northeast Missouri. As a task force member, Detective Feeney received specialized training on the peer-to-peer Ares and Gnutella networks. He explained that a peer-to-peer network is a network made up of individual computers linked together through the Internet to conduct file sharing. Users on the network use file-sharing programs such as Limewire and Frostwire to search for and share image, video, and music files.

Detective Feeney explained that the United States Department of Justice provides a website for ICAC task force members to use in their investigations.¹ Part of the website allows investigators to use the same file-sharing programs and keyword searches used by peer-to-peer file sharers to find child pornography files. A search will return files that are being offered to share along with the IP address of the computer that is offering them.

In this particular case, other ICAC investigators found three files dated February 16, 17, and 20, 2016, that were being offered to share by an IP address. The files were flagged through

¹ The National Internet Crimes Against Children Data System is established by the United States Attorney General to "provide, directly or in partnership with a credentialed law enforcement agency, a dynamic undercover infrastructure to facilitate online law enforcement investigations of child exploitation." 42 U.S.C. § 17615(d)(3)(B)(2012).

the National Center for Missing and Exploited Children as being recognized child pornography based on the SHA1 value of each file. Detective Feeney explained that the SHA1 value is a mathematical algorithm that, because of its length, acts as the DNA or digital fingerprint for a file whether it is an image or video. No two files will have the same SHA1 value; one pixel can be removed from a picture and it will have a completely different SHA1 value than the first. Once the IP address was seen offering files believed to be child pornography based on their SHA1 values, the IP address was “Geo located” to Unionville in Putnam County, which is one of the 13 counties Detective Feeney covers, with an Internet service provider of North Missouri Rural Telephone Company. Based on this information, Detective Feeney obtained and served an investigative subpoena on March 8, 2012, to the Internet service provider to obtain the name and address of the subscriber for the IP address. Shumate was identified as the subscriber.

The trial court denied Shumate’s motion to suppress, and following a bench trial, Shumate was found guilty of three counts of first-degree statutory sodomy, six counts of second-degree statutory sodomy, two counts of second-degree statutory rape, and one count of sexual exploitation of a minor and sentenced to consecutive sentences of three terms of life imprisonment plus fifty-five years. This court affirmed Shumate’s convictions and sentences on direct appeal. *State v. Shumate*, 462 S.W.3d 775 (Mo. App. W.D. 2015).

Thereafter, Shumate filed a timely *pro se* Rule 29.15 motion for postconviction relief. Appointed counsel filed an amended motion on his behalf. The amended motion alleged, in pertinent part, that defense counsel was ineffective for failing to move to suppress all evidence obtained as a result of the government’s wholesale surveillance of peer-to-peer networks, including Shumate’s laptop, and its seizure of Shumate’s IP address from a restricted United States

government website without a prior warrant. The motion court denied Shumate's motion without an evidentiary hearing. This appeal by Shumate followed.

Timeliness of Notice of Appeal

Initially, the State asserts that Shumate's appeal should be dismissed because his notice of appeal, which was filed on March 7, 2016, was untimely. It argues that the judgment denying his postconviction relief motion was entered on January 22, 2016, when the judge signed it and became final thirty days later on February 22, 2016,² rendering his notice of appeal due by March 3, 2016.

The State's assertion is without merit. A notice of appeal must be filed within ten days after a civil judgment becomes final. Rule 81.04(a). If no after-trial motion is filed, a judgment becomes final thirty days after its entry. Rule 81.05(a)(1). "A judgment is entered when a writing signed by the judge and denominated 'judgment' or 'decree' is filed." Rule 74.01(a). Rule 43.02(b) defines "filing" as:

The filing of pleadings and other papers with the court as required by Rules 41 through 101 shall be made by filing them with the clerk of the court, except that a judge may permit the papers be filed with the judge, who shall note thereon the filing date and forthwith transmit them to the office of the clerk.

While the judgment was signed by the judge on January 22, 2016, it was not file-stamped and entered on the docket sheet until January 25, 2016. The judgment was entered on January 25, 2016. *See Federhofer v. State*, 462 S.W.3d 838, 841 n.4 (Mo. App. E.D. 2015)(file-stamp date and date entered on docket sheet rather than date mailed used to determine date of filing of pleading); *Bell-El v. State*, 386 S.W.3d 194, 196 (Mo. App. E.D. 2012)(file-stamp and docket date rather than date judgment was signed used to determine time for appeal); *Escoe v. State*, 131 S.W.3d 447, 449 n.2 (Mo. App. W.D. 2004)(file-stamp date rather than date judgment was signed

² The thirtieth day actually fell on February 21, a Sunday, so is extended to February 22 under Rule 44.01.

used to determine date judgment was entered). The judgment then became final thirty days later on February 24, 2016, and Shumate was required to file his notice of appeal within ten days, or by March 5, 2016. March 5, 2016, however, fell on a Saturday, and under Rule 44.01(a), Shumate had until March 7, 2016, to file his notice of appeal. Shumate's notice of appeal was filed on March 7, 2016, and was, therefore, timely.

Ineffective Assistance of Counsel Claim

In his sole point on appeal, Shumate contends that the motion court clearly erred in denying his Rule 29.15 motion without an evidentiary hearing. He asserts defense counsel was ineffective in failing to move to suppress all evidence obtained as a result of the warrantless search of the ICAC database that provided law enforcement officers with Shumate's IP address, geographical location, and Internet service provider despite lack of prior individualized probable cause.

The judgment of the motion court will be affirmed on appeal unless its findings of fact and conclusions of law are clearly erroneous. Rule 29.15(k); *Johnson v. State*, 406 S.W.3d 892, 898 (Mo. banc 2013). The motion court's judgment is clearly erroneous only if the appellate court is left with a definite and firm impression that a mistake has been made. *Johnson*, 406 S.W.3d at 898.

On a claim of ineffective assistance of counsel, the burden is on the movant to prove by a preponderance of the evidence that (1) counsel failed to exercise the customary skill and diligence of a reasonably competent attorney under similar circumstances and (2) counsel's failure prejudiced him. *Id.* at 898-99 (citing *Strickland v. Washington*, 466 U.S. 668, 687 (1984)). A strong presumption exists that counsel's conduct was reasonable and effective. *Id.* at 899. To show prejudice, the movant must demonstrate a reasonable probability that, but for counsel's errors, the result of the proceeding would have been different. *Id.*

To be entitled to an evidentiary hearing on a motion for postconviction relief, the movant's motion must (1) allege facts, not conclusions, warranting relief, (2) raise factual matters that are not refuted by the file and record, and (3) raise allegations that resulted in prejudice. *Id.* at 898. An evidentiary hearing is not mandatory when the motion and record conclusively show that the movant is not entitled to relief. Rule 29.15(h); *Johnson*, 406 S.W.3d at 898. In this case, to be entitled to an evidentiary hearing on whether defense counsel was ineffective for failing to file a more specific motion to suppress, Shumate had to allege facts, not conclusions, specifying the grounds on which the motion to suppress would have been successful. *Eddy v. State*, 176 S.W.3d 214, 218 (Mo. App. W.D. 2005). Shumate, however, failed to allege facts demonstrating the illegality of the search of the ICAC website.

“The Fourth Amendment guarantees ‘[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizure.’” *Smith v. Maryland*, 442 U.S. 735, 739 (1979)(quoting U.S. CONST. amend. IV). A defendant seeking to suppress evidence based on an alleged unreasonable search must demonstrate that he had a legitimate expectation of privacy in the place searched. *Id.*; *United States v. Stults*, 575 F.3d 834, 842 (8th Cir. 2009); *State v. Woodrome*, 407 S.W.3d 702, 706 (Mo. App. W.D. 2013). This standard involves a two-part inquiry: (1) whether the defendant by his conduct has exhibited an actual (subjective) expectation of privacy and (2) whether his subjective expectation of privacy is one that society is prepared to accept as reasonable. *Id.*

“An individual does not have a legitimate expectation of privacy in items or areas that are exposed to the public, abandoned, or accessed by consent.” *United States v. Giboney*, No. 4:15CR97JAR (SPM), 2016 WL 873325, at *7 (E.D. Mo. Feb. 18, 2016)(citing *Katz v. United States*, 389 U.S. 347, 351 (1967)) (“What a person knowingly exposes to the public, even in his own

home or office, is not a subject of Fourth Amendment protection.”)). “Courts, including the Eighth Circuit, have consistently held that a defendant who shares files on a computer network (even a closed network) has no legitimate expectation of privacy in the shared files.” *Id.* (citing numerous cases). *See also Stults*, 575 F.3d at 842-43, and *United States v. Dodson*, 960 F.Supp.2d 689, 695 (W.D. Tex. 2013)(citing additional cases with such holding).


Shumate contends that the warrantless search of the Department of Justice’s ICAC database for his IP address, the general geographical location of it, and the service provider was unreasonable because Detective Feeney had no individualized suspicion that Shumate was engaged in wrongdoing before searching the database. Citing *United States v. Hall*, No. 2:15-cr-7-FtM-29CM, 2015 WL 5896234 (M.D. Fla. October 7, 2015), Shumate argues that Detective Feeney failed to explain how his IP address and the IP addresses for all the computers being surveilled nationwide was obtained and stored on the Department of Justice database in the first place. In *Hall*, the government had declined to provide any information about the ICAC database or how the defendant’s computer IP address became part of that database. *Id.* at *1. The court stated, “[I]t is reasonable to conclude that someone at some time did something to obtain defendant’s IP address, determined it was associated with child pornography, and placed it in the ICAC database.” *Id.* at *2. The court ordered the government to make sufficient disclosures to enable the defendant to determine how the apparent prior search was conducted and to evaluate the propriety of a motion to suppress. *Id.* Shumate contends that reasonably competent counsel would have filed a motion to suppress all evidence obtained as a result of the warrantless and unreasonable search of the ICAC website and that, had counsel done so, there is a reasonable probability that the court would have suppressed such evidence.

Unlike in *Hall*, the record in this case contains detailed information of the process used by ICAC investigators on the Department of Justice database to obtain IP addresses including Shumate's. Specifically, Detective Feeney testified that the database allows ICAC investigators to use the same file-sharing programs and keyword searches used by ordinary peer-to-peer file sharers to find child pornography files. Other ICAC investigators found three files dated February 16, 17, and 20, 2016, that were being offered to share by an IP address. The files were flagged as being recognized child pornography based on their SHA1 value, or unique digital fingerprint. Once the IP address was seen offering files believed to be child pornography, the IP address was "Geo located" to Putnam County and the Internet service provider was identified. With this information, Detective Feeney obtained and served an investigative subpoena to the Internet service provider and identified Shumate as the subscriber for the IP address.

Contrary to Shumate's argument, Detective Feeney's testimony demonstrated how Shumate's IP address was obtained with the ICAC website, which searches publically available information. Numerous cases have held that law enforcement's use of such software does not violate a defendant's expectation of privacy. *See United States v. Thomas*, 788 F.3d 345, 352 (2nd Cir. 2015)(challenge to reliability of law enforcement's use of software that merely automates the aggregation of public information failed); *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010)(software "functioned simply as a sorting mechanism to prevent the government from having to sift, one by one, through Borowy's already publically exposed files."); *Frazier v. State*, 180 So.3d 1067, 1068-69 (Fla. Dist. Ct. App. 2015)(listing cases holding that expectation of privacy not violated by law enforcement using software that obtained the same information that was available to any other user of the network).

Shumate did not have a reasonable expectation of privacy in the files he shared on a peer-to-peer network and, thus, the task force's use of the ICAC website did not violate the Fourth Amendment. *See Stults*, 575 F.3d at 842-43; *Frazier*, 180 So.2d at 1069. Defense counsel, therefore, had no basis for challenging the procedures used by law enforcement to identify Shumate as the person sharing images of child pornography and was not ineffective for failing to file a more specific motion to suppress. *See Eddy*, 176 S.W.3d at 218 (counsel will not be found to be ineffective for failing to file a meritless motion to suppress). The motion and record conclusively showed that the movant was not entitled to relief, therefore, the motion court did not clearly err in denying Shumate's Rule 29.15 motion without an evidentiary hearing. Point denied.

The judgment is affirmed.



VICTOR C. HOWARD, JUDGE

All concur.